

STATEMENT OF WORK

Date: 1 March 1982

TITLE: Technology Forecast For Computer Security R&D Planning

1. Objective:

The objective of this effort is to identify and forecast trends in the computer technologies which may have an effect on the provision of computer security within the Intelligence Community (IC). Emphasis should be on those technologies which are expected to have significant impact on computing within the next 5 - 10 years. These trends and the factors controlling them will be used to serve as a basis for establishing a computer security R&D plan for the IC.

2. Scope:

This effort shall include a baseline technological assessment of the current state of the computer systems and computer networks technology supporting the Intelligence Community (IC). It shall further identify the technologies which are expected to have a significant impact on computing within the IC as projected over the next 5 - 10 years. Trends in the technologies and in the assimilation and utilization of these technologies shall be forecast. The forecasts shall consider any key security relevant issues and factors which influence these trends in particular as they are applied to the IC. Based on these trends and the forecast for the next 5 - 10 years, the computer security requirements shall be hypothesized. Based on the conclusions and observations, specific R&D initiatives and other computer security efforts may be recommended.

a. Some candidate trends might be:

- rate of advancements in pertinent technical capabilities; e.g., networking, data management, distributed processing, local area support, office automation, etc.

- rate of assimilation of various technologies into the IC inventory, both through establishment of new systems and replacement or enhancement of existing systems.

- rate of increased utilization of and dependence on automated data processing and storage.

b. Some security-relevant issues and factors which might influence the selection and assimilation of the available and emerging technologies into the IC might include: policy restrictions on the use of the technology; cost of achieving security; planned operational requirements; past investments and backward compatibility; etc.

3. Specific Technical Requirements:

a. Perform a baseline technological assessment of the current state of the computer systems and computer networks technology supporting the Intelligence Community (IC).

b. Identify the technologies which are expected to have a significant impact on computing within the IC as projected over the next 5 - 10 years.

c. Perform trends analyses of the technologies identified and of the assimilation and utilization of these technologies in the IC.

d. Prepare a forecast, which considers the key security relevant influences and drivers, of the state of the computer technologies utilized within the IC over the next 5 - 10 years.

e. Hypothesize the computer security requirements, projected over the next 10 years, based on this forecast.

f. Recommend, as appropriate, specific R&D and other computer security initiatives.

4. Milestones:

30 April 1982 (or 2 MOS ADAD):

- Draft of the baseline technological assessment
- Draft Outline of Final Report
- Outline of the methods to be applied for performing the forecast
- List of the technologies selected for the forecast
- List of the security relevant influences and drivers

30 June 1982 (or 4 MOS ADAD):

- Final of the baseline technological assessment
- Final Outline of Final Report
- Draft trend analyses of selected technologies
- Mid effort project status review

31 August 1982 (or 6 MOS ADAD):

- Draft preliminary forecast
- Draft preliminary hypothesis of computer security requirements
- First draft of Final Report

1 October 1982 (or 8 MOS ADAD):

- Final Draft of Final Report
- Final project status review

5. Deliverables:

a. The various drafts and outlines as called for by the Milestones.

b. Final Report which includes (as a minimum):

- 1) Baseline technological assessment
- 2) Forecast methods and selection criteria
- 3) Trends analyses and projections
- 4) Hypotheses, conclusions and recommendations

c. Bimonthly project status reports including accomplishments, problems, milestones/schedule, funds expenditure.

d. Briefing on final report to the members of the Computer Security Subcommittee of NFIIB.

NOTE: Delivery of Final Report due 30 days after completion of the contract.